

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA512

=====  
FreeBSD-SA-26:15.dhclient

Security Advisory  
The FreeBSD Project

Topic: Remotely triggerable out-of-bounds heap write in dhclient

Category: core

Module: dhclient

Announced: 2026-04-29

Credits: Joshua Rogers of AISLE Research Team

Affects: All supported versions of FreeBSD.

Corrected: 2026-04-29 14:47:49 UTC (stable/15, 15.0-STABLE)  
2026-04-29 14:48:29 UTC (releng/15.0, 15.0-RELEASE-p7)  
2026-04-29 14:48:51 UTC (stable/14, 14.4-STABLE)  
2026-04-29 14:49:42 UTC (releng/14.4, 14.4-RELEASE-p3)  
2026-04-29 14:49:24 UTC (releng/14.3, 14.3-RELEASE-p12)  
2026-04-29 14:50:07 UTC (stable/13, 13.5-STABLE)  
2026-04-29 14:50:19 UTC (releng/13.5, 13.5-RELEASE-p13)

CVE Name: CVE-2026-42512

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit <URL:https://security.FreeBSD.org/>.

## I. Background

dhclient(8) is the default IPv4 DHCP client used on FreeBSD. It is responsible for contacting DHCP servers on a network segment and for initialising and configuring network interfaces based on received information.

When processing a DHCP offer, dhclient passes various parameters provided by the server to dhclient-script(8). DHCP options, as documented in dhcp-options(5), are passed via the environment.

## II. Problem Description

As dhclient is building an environment to pass to dhclient-script, it may need to resize the array of string pointers. The code which expands the array incorrectly calculates its new size when requesting memory, resulting in a heap buffer overrun.

## III. Impact

A specially crafted packet can cause dhclient to overrun its buffer of environment entries. This can result in a crash, but it may be possible to leverage this bug to achieve remote code execution.

## IV. Workaround

No workaround is available. Systems not running dhclient(8) are not affected.

The attacker needs to be on the same broadcast domain and respond to DHCP requests. A well-managed network will configure DHCP snooping on switches to prevent rogue DHCP servers from operating.

## V. Solution

Upgrade your vulnerable system to a supported FreeBSD stable or release / security branch (releng) dated after the correction date.

Perform one of the following:

1) To update your vulnerable system installed from base system packages:

Systems running a 15.0-RELEASE version of FreeBSD on the amd64 or arm64 platforms, which were installed using base system packages, can be updated via the pkg(8) utility:

```
# pkg upgrade -r FreeBSD-base
```

2) To update your vulnerable system installed from binary distribution sets:

Systems running a RELEASE version of FreeBSD on the amd64 or arm64 platforms, or the i386 platform on FreeBSD 13, which were not installed using base system packages, can be updated via the freebsd-update(8) utility:

```
# freebsd-update fetch
# freebsd-update install
```

3) To update your vulnerable system via a source code patch:

The following patches have been verified to apply to the applicable FreeBSD release branches.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
# fetch https://security.FreeBSD.org/patches/SA-26:15/dhclient.patch
# fetch https://security.FreeBSD.org/patches/SA-26:15/dhclient.patch.asc
# gpg --verify dhclient.patch.asc
```

b) Apply the patch. Execute the following commands as root:

```
# cd /usr/src
# patch < /path/to/patch
```

c) Recompile the operating system using buildworld and installworld as described in <URL:https://www.FreeBSD.org/handbook/makeworld.html>.

Restart the applicable daemons, or reboot the system.

## VI. Correction details

This issue is corrected as of the corresponding Git commit hash in the following stable and release branches:

Branch/path	Hash	Revision
stable/15/ releng/15.0/	4408b683d237 66d6c32ce7b8	stable/15-n283378 releng/15.0-n281030
stable/14/ releng/14.4/ releng/14.3/	a813012f4b76 d60456d859a1 76734958a098	stable/14-n274077 releng/14.4-n273692 releng/14.3-n271493
stable/13/ releng/13.5/	5d3e93fda7ce 5a5e7883a3bb	stable/13-n259860 releng/13.5-n259216

Run the following command to see which files were modified by a particular commit:

```
# git show --stat <commit hash>
```

Or visit the following URL, replacing NNNNNN with the hash:

<URL:https://cgit.freebsd.org/src/commit/?id=NNNNNN>

To determine the commit count in a working tree (for comparison against nNNNNNN in the table above), run:

```
# git rev-list --count --first-parent HEAD
```

## VII. References

<URL:https://www.cve.org/CVERecord?id=CVE-2026-42512>

The latest revision of this advisory is available at

<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:15.dhclient.asc>

-----BEGIN PGP SIGNATURE-----

```
iQJPBAEBCgA5FiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnySTMbFIAAAAAABAAO
bWFudTIsMi41KzEuMTIsMCwzAAoJEG5Y3pAfABrvvwIP/3DfD428ehRM/ukPC7bY
2AUpIfE5s+AHvE6JiRF8IcbsuVRHsMf01Z6YWYMfPxhzTpoKhjBcC1XuM6fMugcP
9GFRoW1u4f17trfSSTFMbgTA6q7EC1hab1wQsGhpgazQA+lGpUjoISC88ah+jiEu
+Z1b9ubyuYURnstf5V5gj3cRunt9YL3ZuBC0oJJayb0DJSuVvuvvgZL3QvtwSGM98
0JmqEANEY03uGpkbeJsIXBYvzqJdzVHpp/rVF84+PHYLp/uqVaWFlf1WlwEp6wE
0oSKmsWljPjL2bIcbsxu+aJH4XJDwDizgYRq6IVnbV/G3XYqQPJwMyQh/qGDhIq
8hA3tG/aQrs5ukL4WE7eMMM+fNzy+LTBfD3vWyfuabFHmKXBCI+Kc6q+oNcPGXeq
/ofaJav+iv04d0H6XHIJ/MtZ009782EXYWmR8X8E4myZ4z6/vtmqUzL457Kh2v7b
rdGE/1tdd+CyIVobfcuPJBq0cx8Fp8gVydcQ7Ts6i5Hqx/Grz2za5qvQgsHsruqo
ZQxb3rw7J6wp7w7duqEl9cYVZRgz9CdmTsmjCPi8Ws3n00PCBV220/dHBHi/kPtL
f2GPMIBJA2s0HjTiPQJp9LAFaAnUuCsleo4PEj04NDe6QFmT/u1W22AZb050zC0Q
wuVe9dL9HwnNoKuR1hjIWB27
```

=rnNn

-----END PGP SIGNATURE-----